DANIEL J. MULLER, SBN 193396
dmuller@venturahersey.com
VENTURA HERSEY & MULLER, LLP
1506 Hamilton Avenue
San Jose, California 95125
Telephone: (408) 512-3022
Facsimile: (408) 512-3023

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TODD J. RADONSKY, on behalf of himself and all others similarly situated, Plaintiff, v. META PLATFORMS, INC., Defendant.	Case No.: 3:22-cv-6111 **<u>CLASS ACTION COMPLAINT</u>** 1. Violation of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; 2. Violation of the Invasion of Privacy Act, Cal. Penal Code § 630 *et seq.*; 3. Invasion of Privacy (Intrusion Upon Seclusion); 4. Violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*; 5. Unjust Enrichment. **DEMAND FOR JURY TRIAL**

Plaintiff Todd J. Radonsky, on behalf of the Class defined below, brings this action against Meta Platforms, Inc. and alleges as follows:

INTRODUCTION

1. This class action is filed on behalf of, and seeks relief for, all persons who used Meta's Facebook, Instagram, and/or Messenger app and whose private browsing activity and communications were surreptitiously intercepted, monitored and recorded by Meta's in-app internet browsers.

2. In April 2021, Apple's iOS 14 update required Meta to obtain its users' informed consent before tracking their internet activity on apps and third-party websites. As a result, Meta lost access to its primary stream of revenue, which it derived from the user data it obtained from this tracking.

3. Now, even when users do not consent to being tracked, Meta tracks Instagram and Facebook users' online activity and communications with external third-party websites by injecting JavaScript code into those sites.

4. When a user clicks on a web link within the Facebook, Instagram, or Messenger app, Meta automatically directs them to the in-app browser Meta monitors instead of the user's default browser. Meta does not tell its users this is happening or explain that they are being tracked.

5. The user information Meta intercepts, monitors, and records includes personally identifiable information, private health details, text entries, and other sensitive confidential information.

6. Meta's undisclosed tracking of users' browsing activity and communications violates federal and state wiretap laws and other laws, entitling Plaintiff and Class members to damages.

7. Plaintiff and Class members also seek injunctive relief and equitable remedies to stop Meta's undisclosed and non-consensual tracking.

JURISDICTION AND VENUE

8. The Court has personal jurisdiction over Defendant Meta Platforms, Inc. because it is headquartered in this District.

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises in part under federal law—the Wiretap Act, 18 U.S.C. § 2510 *et seq.*—and pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, the amount in controversy exceeds

$5 million (excluding interest and costs), and at least one Class member is a citizen of a state different from the state in which Meta is headquartered.

10. Pursuant to 28 U.S.C. § 1391, venue is proper because Meta is headquartered in this District.

DIVISIONAL ASSIGNMENT

11. Pursuant to Civil Local Rule 3-2(c), a substantial part of the events giving rise to the Plaintiff's and Class members' claims occurred in San Mateo County, California. Consequently, this action should be assigned to the San Francisco or Oakland Divisions of this Court.

PARTIES

12. Plaintiff Todd J. Radonsky is a resident of Los Angeles County, California. Mr. Radonsky has had active Facebook and Instagram accounts for many years and regularly accesses his accounts using the Facebook and Instagram Apps on his iPhone. Using the systematic process described below, Meta tracked and intercepted Mr. Radonsky's specific electronic activity and private communications with external third-party websites without his knowledge or consent. Mr. Radonsky reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta, based on, among other things, Meta's representation that it would not track users' online activity without their permission.

13. Meta Platforms Inc. (d/b/a Meta; f/k/a Facebook, Inc.) is a Delaware Corporation headquartered in Menlo Park, California. Meta is a multinational technology conglomerate that owns Facebook and Instagram, among other social media platforms, and offers a wide array of products and services, including advertising and marketing.

FACTUAL ALLEGATIONS

A. Meta's Longstanding History of Exploiting Users' Private Information for Profit

14. Meta is the owner and operator of two of the largest social media platforms in the world: Facebook and Instagram.

15. Meta generates revenue primarily by selling advertisement space on those same two social media platforms—Facebook and Instagram.

16. To attract and entice businesses to advertise on Facebook and Instagram, Meta collects and aggregates information from users of those platforms, which enables businesses to target their social media advertisements to specific user profiles/preferences.

17. Although Meta does not require Facebook and Instagram users to pay a monetary subscription fee, membership is not free. Instead, Meta conditions the use of Instagram and Facebook upon users disclosing sensitive and valuable personal information when they register, including birthdates and email addresses, and surreptitiously gathers and collects information related to their preferences, likes, dislikes, and tendencies.

18. The personal information Meta collects has substantial economic value. One study valued users' web-browsing histories at $52 per year.

19. Meta's sale of digital advertising space accounted for 97% of its revenue in 2021. Meta's business model heavily relies on its collect and analyze information that reveals users' individual preferences, dislikes, and habits in order to then leverage that information to generate profits by tailoring advertising to individual targeted users.

20. Meta's financial success thus is the result of connecting advertisers with its massive repository of personal data it gathers from its users. Meta maximizes its profits by targeting ads to individuals who algorithms have determined may be personally interested in certain advertised product or service. Meta collects extensive data about its users, continuously aggregates and analyzes this data, and deploys it to offer targeted advertising services to advertisers.

21. Meta's business model, which depends on its ability to collect and gather its users' information, has resulted in repeated violations of user privacy rights over the years. Meta's tactics when designing its social media platforms have always been aimed at data mining, and its use of plug-ins, cookies, Facebook Beacon, the Facebook Like Button, Facebook Pixel, and related tools have led to dozens of private lawsuits and federal investigations.

22. Meta has also shared its users' private messages and the details relating to their personal contacts without user consent. From 2010 to 2018, Facebook allowed more than 150 third parties, including Amazon, Microsoft, Netflix, and Spotify, to access and utilize this private information.[1] And in 2019, Facebook agreed to pay a $5 billion penalty and submit to new restrictions and a modified corporate structure to settle Federal Trade Commission charges that Facebook violated a 2012 FTC Order by deceiving users about their ability to control the privacy of their personal information.[2]

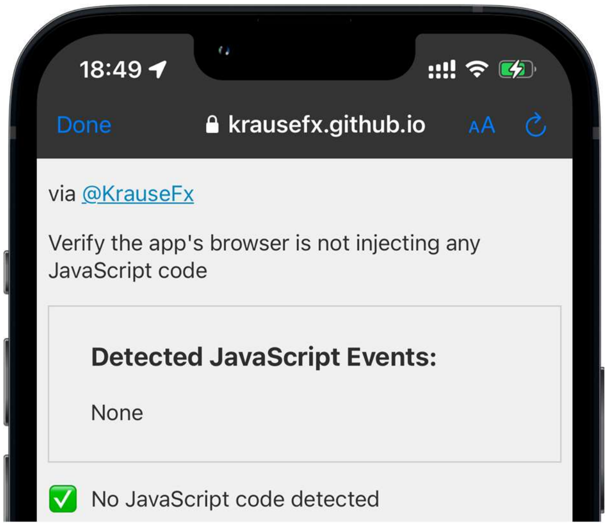
B. Meta Intentionally Manipulated Third-Party Websites and Injected JavaScript Into its In-App Browser to Track User Activity Without Their Knowledge or Consent

23. Data privacy researcher and former Google engineer, Felix Krause, published a recent report revealing that Meta implemented and maintains a practice of injecting code into third-party websites, which enables it to track users and intercept data that would otherwise be unavailable to it. If a user accessed the same third-party website from their own web browser, such as Google Chrome or the Safari app, Meta would not be able to track and intercept the users' communications with that website.

24. Krause developed www.InAppBrowser.com as a tool that can determine whether a particular in-app browser is injecting JavaScript code into third-party websites. This tool is essential for distinguishing Meta's practices from its competitors and demonstrates that Meta is actively using JavaScript code to undermine its users' privacy preferences. The image below demonstrates what happens when a user clicks on a web link from within Telegram, a popular messaging app that does not inject JavaScript Code onto third-party websites but still prompts users its own in-app browser instead of their default browser when users follow a hyperlink:

[1] https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (last visited October 17, 2022).

[2] https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (last visited October 17, 2022).



via @KrauseFx

Verify the app's browser is not injecting any JavaScript code

Detected JavaScript Events:

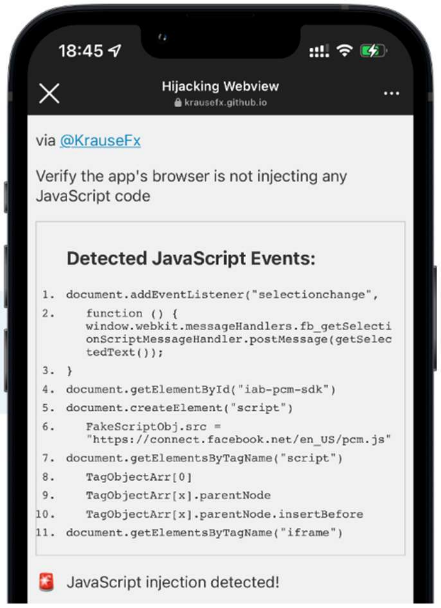
None

✅ No JavaScript code detected

As demonstrated by the image above, no JavaScript events were detected, which indicates that Telegram properly prompts its users to use its in-app browser, but it does not track users' activity on or communications with third-party web pages.

25. Conversely, the images below demonstrate what happens when the same third-party web link is clicked on from within the iOS Facebook (left) and Instagram (right) apps:

Facebook App:



via @KrauseFx

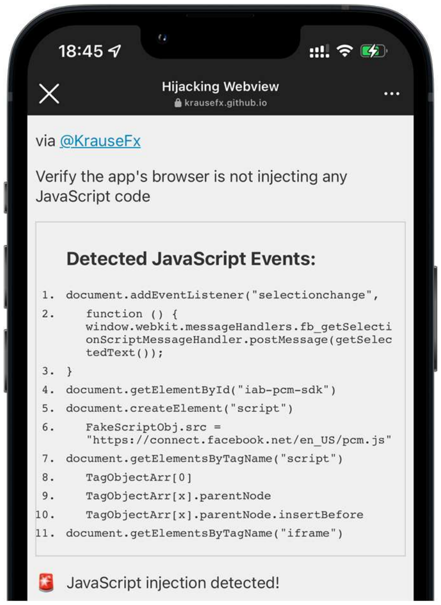
Verify the app's browser is not injecting any JavaScript code

Detected JavaScript Events:

```
document.addEventListener("selectionchange",
   function () {
   window.webkit.messageHandlers.fb_getSelecti
   onScriptMessageHandler.postMessage(getSelec
   tedText());
}
document.getElementById("iab-pcm-sdk")
document.createElement("script")
   FakeScriptObj.src =
   "https://connect.facebook.net/en_US/pcm.js"
document.getElementsByTagName("script")
   TagObjectArr[0]
   TagObjectArr[x].parentNode
   TagObjectArr[x].parentNode.insertBefore
document.getElementsByTagName("iframe")
```

JavaScript injection detected!

Instagram App:



via @KrauseFx

Verify the app's browser is not injecting any JavaScript code

Detected JavaScript Events:

```
document.addEventListener("selectionchange",
   function () {
   window.webkit.messageHandlers.fb_getSelecti
   onScriptMessageHandler.postMessage(getSelec
   tedText());
}
document.getElementById("iab-pcm-sdk")
document.createElement("script")
   FakeScriptObj.src =
   "https://connect.facebook.net/en_US/pcm.js"
document.getElementsByTagName("script")
   TagObjectArr[0]
   TagObjectArr[x].parentNode
   TagObjectArr[x].parentNode.insertBefore
document.getElementsByTagName("iframe")
```

JavaScript injection detected!

26. The foregoing images show that when the same website is opened from the iOS Facebook and Instagram apps, several different JavaScript events are detected and identified indicating that Meta is purposely injecting JavaScript code onto third-party web pages.

27. Krause's report, entitled "*iOS Privacy: Instagram and Facebook can Track Anything you do on any Website in their In-App Browser*," describes how Meta uses JavaScript to alter websites and override its users' default privacy settings by directing users to Instagram's and Facebook's in-app browsers instead of their pre-programmed default web browser.[3]

28. Injecting JavaScript into the code of third-party websites can allow a malicious actor to intercept confidential information communicated to those sites:[4]

> **What is a JavaScript Injection Attack?**
> A JavaScript injection attack is a type of attack in which a threat actor injects malicious code directly into the client-side JavaScript. This allows the threat actor to manipulate the website or web application and collect sensitive data, such as personally identifiable information (PII) or payment information.

29. Meta is using this tool to gain an advantage over its competitors and, with respect and unbeknownst to iOS users, to intercept and track their communications with third-party websites. Meta inserts code to track its users' in-app browsing activity without their knowledge or consent, even when users have declined to "opt in" to Meta's tracking and set their devices to block third-party tracking cookies.

C. Meta Intentionally Overrides Users' Privacy Settings to Intercept and Track its Users' Private Interactions and Communications with Third-Party Websites

30. While using the Instagram or Facebook app, if users click on a link to an external website contained within the app, Meta *automatically* reroutes the user to Meta's own in-app web browser instead of the users' built-in web browser (such as the Safari app that is preloaded onto iPhones or web browser apps downloaded by users, such as Google Chrome). As a result, third-party websites are rendered *inside* the Instagram or Facebook app and the user who clicked the link navigates that page

[3] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last visited October 17, 2022).

[4] https://www.feroot.com/education-center/what-is-a-javascript-injection-attack/ (last visited October 17, 2022).

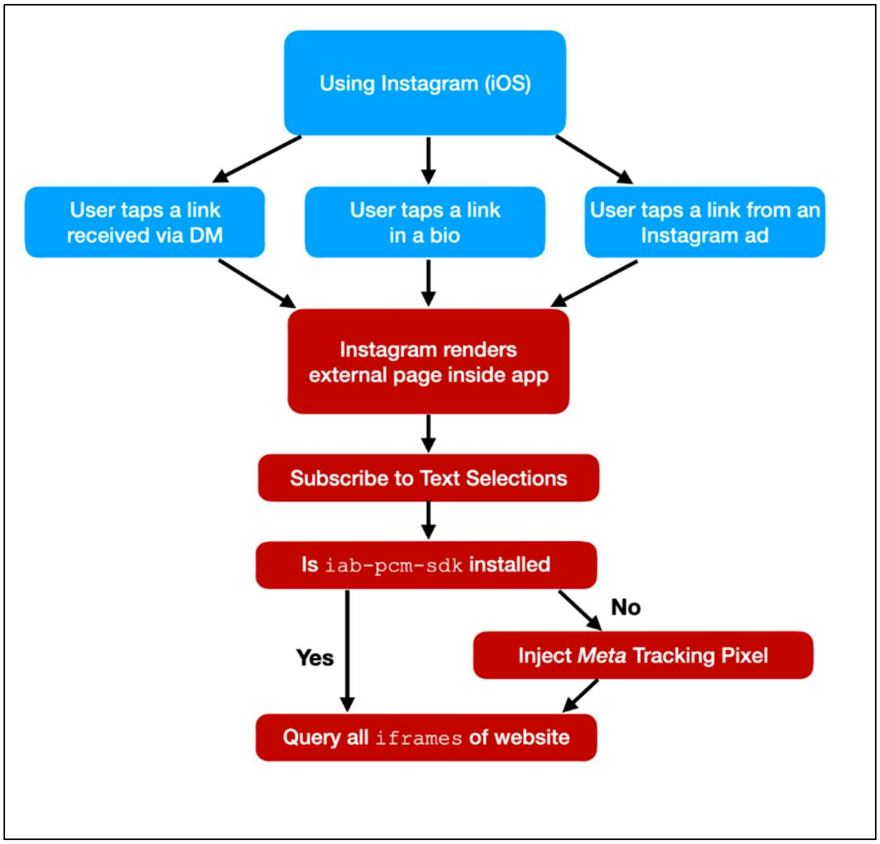
through the Instagram or Facebook internal browser. That enables Meta "to monitor everything happening on external websites, without the consent from the user, []or the website provider."[5]

31. Specifically, the Instagram or Facebook app injects Meta's JavaScript code into every third-party website a user visits from within Instagram's or Facebook's in-app browser, which allows Meta to then intercept, monitor and record its users' interactions and communications with third parties, providing data to Meta that it aggregates, analyzes, and uses to boost its advertising revenue.

32. When this occurs, Meta never notifies Instagram or Facebook users through readily available means like, for instance, a pop-up window or other prominent means, that Meta is tracking their browser activity. The "Off-Facebook activity" settings tab within the Facebook app (and Instagram equivalent) does not disclose the practice. At no point does Meta fairly or reasonably disclose to users its practice of intercepting, monitoring, and selling their activities and communications while using its in-app browser. Moreover, many users are unaware that they are accessing third-party websites from within Meta's in-app browser because the appearance and functionality of the in-app browser mimics that of any other browser.

33. As demonstrated in Figure 3 below, this systematic process occurs whenever a user clicks on a link they received in their inbox (through the private messaging feature) or when they click on a link displayed on the common areas of Instagram and Facebook, including other users' posts, accounts, and content. While the following flowchart refers to "Instagram," the same process occurs in the Facebook in-app browser and Messenger in-app browser:

[5] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last visited October 17, 2022).


Using Instagram (iOS)
User taps a link received via DM
User taps a link in a bio
User taps a link from an Instagram ad
Instagram renders external page inside app
Subscribe to Text Selections
Is iab-pcm-sdk installed
No
Yes
Inject Meta Tracking Pixel
Query all iframes of website

The image above depicts the systematic manner in which Meta injects JavaScript into external third-party webpages for the purpose of intercepting, tracking, monitoring, and collecting data about its users' interactions with external third-party webpages.

34. This JavaScript injection practice enables Meta to surveil and extract details about its users' text selections and other communications with third-party websites:

> This, in combination with listening to screenshots, gives Meta full insight over what specific piece of information was selected & shared. The [Meta] app checks if there is an element with the ID iab-pcm-sdk: According to this tweet, the iab likely refers to "In App Browser". If no element with the ID iab-pcm-sdk was found, [Meta] creates a new script element, sets its source to https://connect.facebook.net/enUS/pcm.js. It then finds the first script element on [the] website to insert the pcm JavaScript file right before [Meta] also queries for iframes on [the] website.[6]

Thus, by running custom scripts on third-party websites, Meta can and does intercept, view, monitor, and record all user interactions—every button and link they tap, as well as text selections, screenshots,

[6] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last visited October 17, 2022).

form inputs (including passwords, addresses, and payment card numbers), other personally identifiable information, protected health details, and other private and confidential communications and data.

D. Meta's In-App Tracking Process and Acknowledgement that it Tracks Users' Browser Activity

35. Meta acknowledged that it tracks Instagram's and Facebook users' in-app browsing activity within hours of the practice being reported to Meta in connection with its "Bug Bounty Program." Meta later stated that the data obtained through this practice assists in "aggregating events" before such "events" are deployed in targeted advertising.

36. In contrast, Meta has not implemented this JavaScript code injection practice on the in-app browser of another of its properties, WhatsApp. This disparity in business conduct confirms that injecting JavaScript is not necessary for users' security or for any other legitimate purpose. Instead, used on Instagram and Facebook, this practice serves only to benefit Meta and increase its revenue from ad impressions sold for display to Instagram and Facebook users.

37. Meta's injection of JavaScript coincides with recent privacy updates for iPhones and other iOS devices. In 2020, Apple announced that beginning in 2021, it would change how its iOS mobile operating systems handle users' privacy preferences, thereby requiring apps to obtain users' affirmative consent prior to being tracked across application or on external websites. After this Apple announcement, Meta began "waging a public relations effort to attack Apple ahead of new iOS data privacy changes that would make it harder for advertisers to track users, in a possible sign of just how much the social network views the move as a threat to its core business."[7]

38. Facebook held press conferences and ran advertisements critical of Apple's decision to require affirmative user consent: "In ads featured in The New York Times, Wall Street Journal and Washington Post, Facebook slammed Apple's upcoming requirement for users to give explicit permission for apps to track them across the internet. Facebook said the move could be 'devastating' to millions of small businesses that advertise on its platform."[8] WhatsApp likewise "criticized Apple over

[7] https://edition.cnn.com/2020/12/16/tech/facebook-apple-ios-privacy-rules/index.html (last visited October 17, 2022).

[8] *Id.*

its move to display a summary of an app's privacy practices before a user downloads it from the App Store, almost like a nutrition label for data collection."[9]

39. In response, Apple stated in part, "We believe that this is a simple matter of standing up for our users. Users should know when their data is being collected and shared across other apps and websites, and they should have the choice to allow that or not."[10] Apple also noted that "App Tracking Transparency in iOS 14 does not require Facebook to change its approach to tracking users and creating targeted advertising, it simply requires they give users a choice."[11]

40. As of May 2021, shortly after Apple introduced iOS 14.5, 96% of Apple users in the United States had not consented to being tracked by apps on their iPhone. "According to [Meta], empowering Apple's users to opt out of tracking cost the company $10,000,000,000 in the first year, with more losses to come after that."[12] Hence "[w]ith web browsers and iOS adding more and more privacy controls into the users' hands, it becomes clear why [Meta] is interested in monitoring all user web traffic of external websites."[13]

41. Meta began showing its users a screen that described the consequences of iOS 14.5 and the long-term impact it could have on Meta's ability to provide apps and software. Through these and related communications strategies, Meta was "threatening that users will need to pay for their services. But only if users don't allow the pair to track them from app to app after installing iOS 14.5."[14]

E. Meta's Tracking Practices and Associated Conduct Have Harmed Plaintiff and Class Members

42. Meta does not inform Facebook and Instagram users that clicking on links to third-party websites from within Facebook and Instagram automatically send the user to Instagram's or Facebook's in-app browser, as opposed to the user's default web browser, or that Meta will monitor the user's

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] https://www.eff.org/deeplinks/2022/06/facebook-says-apple-too-powerful-theyre-right (last visited October 17, 2022).

[13] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last visited October 17, 2022).

[14] https://www.imore.com/facebook-and-instagram-threaten-charge-access-ios-145-unless-you-give-it-your-data (last visited October 17, 2022).

activity and communications while on those sites. Because nothing alerts users as to these facts, they are unaware of the tracking; most do not even realize they are browsing the third-party website from within Instagram's and Facebook's in-app browsers. Therefore, users freely engage with these sites, sharing all manner of personal facts and preferences, without having reason to know they are being tracked or are actually still within Instagram's or Facebook's app.

43. Even users who may realize they are visiting websites from within Instagram's and Facebook's in-app browsers do not realize that this activity overrides their privacy settings and enables Meta to track, intercept, and monitor their activities on the websites due to Meta's undisclosed injection of code. Meta's JavaScript injection cannot be detected by a lay person, and a website when viewed on Instagram's or Facebook's in-app browser functions no differently than it would otherwise.

44. Users also reasonably expect that their communications with external third-party websites are not being intercepted and tracked because their default browser disables and blocks third-party cookies. Meta does not inform users that its in-app browser differs from Safari and other default browsers regarding such privacy settings.

45. Moreover, Meta fails to disclose the consequences of browsing, navigating, and communicating with third-party websites from within Instagram's and Facebook's in-app browsers—namely, that doing so overrides their default browser's privacy settings, which users rely on to block and prevent tracking. Similarly, Meta conceals the fact that it injects JavaScript that alters external third-party websites so that it can intercept, track, and record data that it otherwise could not access.

46. Plaintiff and the Class reasonably believed that his communications and interactions with third-party websites were confidential—solely between themselves and external websites. Had they known that Meta could and would use its in-app browser to overcome their default browser settings and override their privacy choices, Plaintiff and the Class would have avoided navigating to third-party websites from within Instagram and Facebook. Instead, they would have copied and pasted links into standard browser to avoid being tracked, and ensured that their communications with third-party websites were made outside of Instagram's and Facebook's in-app browsers, particularly when the communications involved sensitive or other personally identifiable information, such as private health or other confidential information.

CLASS ACTION ALLEGATIONS

47. Plaintiff brings this lawsuit under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3) as representative of the following Class and Subclass:

> Class: All persons in the United States with active Instagram and/or Facebook accounts who visited a third-party external website on Instagram's or Facebook's in-app browser during the Class Period.
>
> iOS Subclass**:** All persons with active Instagram and/or Facebook accounts who, using an iOS device, visited a third-party external website on Facebook's in-app browser during the Class Period.

Plaintiff reserves the right to modify these definitions and/or to propose additional subclass as appropriate based on further investigation and discovery.

48. The "Class Period" is the time period beginning on the date that Meta began implementing on Instagram and/or Facebook the practices described in the Complaint and ending on the date of entry of judgment.

49. Meta and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling are excluded from the Class. Excluded from the Class are persons employed by counsel in this action and any judge to whom this case is assigned, his or her spouse and immediate family members, and members of the judge's staff.

50. Numerosity. The members of the Class are so numerous that joinder of all members would be impracticable. The exact number of Class members is unknown to Plaintiff at this time, but it is estimated to number at least in the tens of millions. The identity of Class members is readily ascertainable from Meta's records.

51. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff used Meta's platforms to view third-party websites that were embedded as URLs within the respective Meta applications, and all Class members were similarly affected by Meta's wrongful conduct related thereto.

52. Adequacy. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff's interests are coincident with, and not antagonistic to, those of the Class members. Plaintiff is represented by attorneys experienced in the prosecution of class action litigation generally,

and in digital privacy litigation specifically, who will vigorously prosecute this action on behalf of the Class.

53. Common Questions of Law and Fact Predominate. Questions of law and fact common to the Class members predominate over questions that may affect only individual Class members because Meta has acted on grounds generally applicable to the Class. The following questions of law and fact are common to the Class and predominate over any individual issues, among others:

a. Whether Meta intentionally tapped the lines of electronic communication between Class members and third-party websites they visited;

b. Whether Instagram's or Facebook's in-app web browsers surreptitiously record Class members' private communications and personally identifiable information;

c. Whether Class members have a reasonable expectation of privacy with respect to such information;

d. Whether Meta's invasion of Class members' privacy rights is highly offensive to a reasonable person;

e. Whether Meta violated state and federal laws by tracking Internet use and intercepting its users' communications when they visited third-party websites;

f. Whether Meta's conduct resulted in a breach of confidentiality;

g. Whether Meta's statements and omissions misled Class members as to the level of control they had over their private communications derived from activity on the Instagram or Facebook app; and

h. Whether Class members are entitled to damages, restitution and/or injunctive relief.

54. Superiority. A class action will permit numerous similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication of evidence, effort, or expense. A class action will provide Plaintiff and Class members a method for obtaining redress on claims that could not practicably be pursued individually. Plaintiff is not aware of and does not anticipate any manageability or other issue that would preclude maintenance of this case as a class action.

55. Rule 23(b)(1) and (b)(2) Certification. Class certification is also appropriate under Rules

23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Meta;

b. The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impeded their ability to protect their interests; and

c. Meta has acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole.

FIRST CLAIM FOR RELIEF
VIOLATION OF THE WIRETAP ACT
18 U.S.C. § 2510 *et seq.*
(On Behalf of the Class)

56. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

57. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986, prohibits the intentional interception of any wire, oral, or electronic communication.

58. Pursuant to 18 U.S.C. § 2520(a), any person whose wire, oral or electronic communication is intercepted has a private right of action thereunder.

59. Without Plaintiff and Class members' knowledge or consent, Meta intercepted the contents of their electronic communications when they navigated from Facebook and/or Instagram to third-party websites.

60. Plaintiff and Class members were unaware that Facebook and/or Instagram were intercepting and tracking their electronic communications and interactions with third-party websites.

61. Meta intentionally used technology—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff' and Class members' electronic communications, in violation of the Wiretap Act.

62. Plaintiff and Class members are persons whose electronic communications were intercepted within the meaning of Section 2520. As such, they are entitled to preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual damages, punitive damages, and reasonable attorneys' fees and costs of suit.

<u>SECOND CLAIM FOR RELIEF</u>
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, Cal. Penal Code § 630 *et seq.*

63. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

64. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630-638. The Act contains the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

65. California Penal Code § 631(a) accordingly provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

66. At all relevant times, Meta's practice of injecting JavaScript allowed it to access, intercept, learn the contents of and collect Plaintiff and Class members' personally identifiable information and other confidential data, including information concerning their interactions with third-party websites, even when Plaintiff and Class members' default internet browsers and devices were set to block such actions.

67. Plaintiff, and each Class Member, during one or more of their interactions on the internet during the Class period, communicated with one or more third-party websites owned by entities based

in California, or with one or more entities whose servers were located in California. Communications from the California web-based entities to Plaintiff and Class members, and from Plaintiff and Class members to the California web-based entities, were sent to California.

68. Plaintiff and Class members did not consent to any of Meta's actions in intercepting, reading, and learning the contents of their communications with such California-based entities. Meta read and learned the contents of Plaintiff and Class members' communications in transit and in an unauthorized manner. Meta failed to disclose that it was intercepting, tracking and learning the contents of such private conversations and activities when users visit external third-party websites from within the Instagram or Facebook apps.

69. Meta's conduct was intentional in that it purposefully installed code which allows it to eavesdrop and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta. Meta directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiff, Class members and California-based web entities.

70. The information Meta intercepts while Plaintiff and Class members are using its in-app browser includes personally identifiable information and other highly specific, confidential information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on the website.

71. Plaintiff and Class members have suffered loss by reason of these violations, including but not limited to, violation of their right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

72. As a result of the above violations and pursuant to CIPA section 637.2, Meta is liable to Plaintiff and Class members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 provides "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

73. Plaintiff further requests, as provided under CIPA, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

THIRD CLAIM FOR RELIEF
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Class)

74. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

75. Plaintiff and Class members had a reasonable expectation of privacy when communicating with third-party websites, and, as a result of Meta's actions, they have suffered harm and injury, including from the invasion of their privacy rights.

76. By intercepting Plaintiff and Class members' wire and electronic communications on the internet, Meta intentionally intruded upon their solitude or seclusion.

77. Meta's intentional intrusion on Plaintiff's solitude or seclusion is highly offensive to a reasonable person, especially considering the highly personal, sensitive, and confidential information and data that Meta monitored, intercepted, transmitted and recorded.

78. Meta's conduct infringed Plaintiff and Class members' privacy interests in (1) preventing the dissemination and/or misuse of their sensitive, confidential personally identifiable information; (2) maintaining control over the type of information that Meta tracks and/or records; and (3) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, without limitation the right to visit and interact with various internet sites without that information being intercepted by Meta without Plaintiff's and Class member knowledge or consent.

79. Plaintiff and Class members have been damaged as a direct and proximate result of Meta's invasion of their privacy rights and are entitled to just compensation, including monetary damages.

FOURTH CLAIM FOR RELIEF
VIOLATION OF THE UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200 *et seq*., ("UCL")

80. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

81. By engaging in the acts and practices described herein, Meta has committed one or more acts of unfair competition within the meaning of the UCL, and as a result, Plaintiff and the Class members have suffered injury in fact and lost money and/or property, namely, as described herein, the insertion of JavaScript on their devices and the invasion and lost value of their personally identifiable information and other confidential data.

82. Meta's conduct violates federal and state law and, therefore, the unlawful prong of the UCL. Further, Meta's conduct is substantially unfair, predatory and contrary to California's legislatively declared public policy in favor of protecting the privacy and security of personal confidential information.

83. Plaintiff interacted with various third-party websites reasonably believing that their browsing activities—and any facts and information communicated to third-party websites—were secure and confidential (i.e., solely between himself and the third-party website). In actuality, without Plaintiff or Class members' knowledge or consent, Meta injected code into every web URL accessed through the in-app browser, which was capable of altering security and privacy settings previously set by Plaintiff and Class members. Through this conduct, Meta actively intercepted, viewed, and collected Plaintiff' and Class members' personally identifiable information so that it could be used for Meta's financial benefit. The information and data Meta intercepted includes highly sensitive and valuable personal information, including but not limited to personally identifiable information, confidential medical information, and other confidential communications and facts.

84. There is no justification for Meta's conduct other than to increase, beyond what it would have otherwise realized, its revenues from third parties and the value of its information assets through the acquisition and sale of Plaintiff's and Class members' personal information. Meta's conduct lacks justification in that Meta has benefited from such conduct and practices while Plaintiff and Class members have been misled as to the nature and integrity of Meta's services and have, in fact, suffered material disadvantage as to their interests in the privacy and confidentiality of their personal information. Meta's conduct offends public policy in California as embodied in the Consumers Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them to safeguard their privacy interests, including Cal. Civ.

Code § 1798.80.

85. Meta's acts and practices were fraudulent in violation of the UCL because they were likely to, and did, in fact, mislead the members of the public to whom they were directed. Meta actively concealed its illegal tracking practices and had exclusive knowledge of them, creating a duty to disclose. Meta failed to disclose these practices and disclosing them would have been a material and important factor in Plaintiff and Class members' actions with respect to visiting third-party websites through Instagram's or Facebook's in-app browser or another browser. Meta's surreptitious and deceptive tracking practice to profit from their data caused the data to lose value.

86. Plaintiff, on behalf of himself and the Class, accordingly seeks restitution, injunctive relief, and such other relief that is available and warranted under the UCL.

FIFTH CLAIM FOR RELIEF

UNJUST ENRICHMENT

(On Behalf of the Class)

87. Plaintiff incorporates the above allegations by reference as if fully set forth herein and brings this count individually and on behalf of the Class.

88. Plaintiff and Class members conferred benefits on Meta by using Instagram and/or Facebook and unknowingly providing access to their personal and confidential information, including through Meta's illegal and undisclosed tracking practices detailed above.

89. Meta secretly intercepts, monitors, and records Instagram and Facebook users' online activity and communications with external third-party websites by injecting code into those sites. When users click on a link within the Instagram or Facebook app, Meta automatically directs them to the in-app browser that it is monitoring, rather than to their standard browser, without telling the user this is happening or that they are being tracked, even where users have not consented to being tracked and their other relevant settings would block such tracking.

90. Under these circumstances, equity and good conscience militate heavily against permitting Meta to retain the profits and benefits from its wrongful conduct. They should accordingly be disgorged or placed in a constructive trust so that Plaintiff and Class members can obtain restitution.

PRAYER FOR RELIEF

91. WHEREFORE, Plaintiff, on behalf of himself and the Class defined herein, respectfully requests that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiff and Plaintiff's attorneys to represent the Class;

B. Award compensatory damages, including statutory damages where available, and/or restitution to Plaintiff and the Class against Meta in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Meta, and its officers, agents, servants, employees and attorneys, from injecting JavaScript onto its users' devices in a manner that allows Meta to intercept users' private communications and track users' internet activity on third-party websites in a manner that is inconsistent with the privacy settings enabled by users' ordinary web browsers and/or inconsistent with users' decision to opt-out of tracking;

D. Award Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant such other and further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

92. Plaintiff hereby demands a trial by jury for all claims so triable.

DATED: October 17, 2022. **VENTURA HERSEY & MULLER, LLP**

BY: */s/ Daniel J. Muller*
DANIEL J. MULLER, SBN 193396
dmuller@venturahersey.com
VENTURA HERSEY & MULLER, LLP
1506 Hamilton Avenue
San Jose, California 95125
Telephone: (408) 512-3022
Facsimile: (408) 512-3023

Joseph G. Sauder
Mark B. DeSanto
SAUDER SCHELKOPF
1109 Lancaster Avenue
Berwyn, PA 19312

Telephone: (888) 711-9975
Facsimile: (610) 421-1326
jgs@sstriallawyers.com
mbd@sstriallawyers.com
Daniel O. Herrera
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
150 S. Wacker Dr., Suite 3000
Chicago, Illinois 60606
Phone: (312) 782-4880
Facsimile: (312) 782-4485
bclobes@caffertyclobes.com
dherrera@caffertyclobes.com

Bryan L. Clobes
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
205 N. Monroe St.
Media, PA 19063
Tel. (215) 864-2800
Fax (215) 964-2808
bclobes@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class